# TECHNIQUE T816: DEVICE RESTART/SHUTDOWN

| CyOTE Use Case(s) | MITRE ATT&CK for ICS® Tactic |
|---|---|
| Alarm Logs, HMI, Remote Login | Inhibit Response Function |
| **Data Sources** | |
| **Potential Data Sources** | Network Scan, Packet Capture, Device and Application Logs, Alarm History, Asset Management |
| **Historical Attacks** | Industroyer/CRASHOVERRIDE[1] |

## TECHNIQUE DETECTION

The Device Restart/Shutdown technique[2] (Figure 1) may be detected when a device shuts down and restarts unexpectedly.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[3] and Recipes[4] for asset owners and operators (AOO) to identify indicators of attack for techniques like Device Restart/Shutdown within their operational technology (OT) networks. Referencing CyOTE Case Studies[5] of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

## PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS

The Device Restart/Shutdown technique was used in the Industroyer attack in the Ukraine in 2016.[6,7] In this attack, the following observables were identified:

- Device restarts and shutdowns recorded as events
- Alarms for shut down or restarted devices
- Increased internet traffic

*Disclaimer: Past occurrences are not guaranteed to occur in future attacks.*

---

[1] MITRE, Software: Industroyer, CRASHOVERRIDE, https://collaborate.mitre.org/attackics/index.php/Software/S0001
[2] MITRE ATT&CK for ICS, T816: Device Restart/Shutdown, https://collaborate.mitre.org/attackics/index.php/Technique/T0816
[3] A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.
[4] A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.
[5] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.
[6] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
[7] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

## COMPREHENSION

In the Industroyer attack, devices were shut down and restarted once the adversary had enumerated the network and gained access to the Data Historian to initiate the compromise. Industroyer includes a module that renders a device unresponsive, forcing manual restart. The adversary used this technique to support Manipulation of View, preventing operators from knowing what was happening in the system, and thus was able to cause impactful and damaging changes to the system.[8] By understanding the nature and possible origins of this attack, as well as how the adversary used the Device Restart/Shutdown technique to execute the attack, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

## CURRENT CAPABILITY

Two CyOTE Proof of Concept tools were developed to help identify any time a system is shutdown or restarted. One tool parses Windows event logs to identify IDs representing device restarts and shutdowns; the other tool parses Linux utmp records to identify restarts and shutdowns.

## POTENTIAL ENHANCEMENTS

These CyOTE Proof of Concept tools can be tailored to use multiple methods to track device restarts and shutdowns. Correlating these various methods, the operational tools will attempt to identify the initiation of a shutdown or reboot and classify it as malicious or authorized. When an alert is identified, the tools can support customizable alerting (e.g., outputting a syslog entry or STIX 2.1 formats).

## ASSET OWNER DEPLOYMENT GUIDANCE

Fully developed operational tools should be installed on individual devices where system information can be collected and analyzed by the operational tools. The operational tools could also be deployed in a reduced capacity to remotely connect to individual devices and collect available logs.

*AOOs can refer to the CyOTE Technique Detection Capabilities report (visit https://inl.gov/cyote/) for more information on the background and approach of CyOTE's technique detection capabilities.*

*AOOs can also refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.*

| | |
|---|---|
| **Click for More Information** | CyOTE Program \|\| Fact Sheet \|\| CyOTE.Program@hq.doe.gov |
| **DOE Senior Technical Advisor** | Edward Rhyne \|\| Edward.Rhyne@hq.doe.gov \|\| 202-586-3557 |

[8] CyOTE Case Study: CRASHOVERRIDE/Industroyer. Visit https://inl.gov/cyote/ for more information.

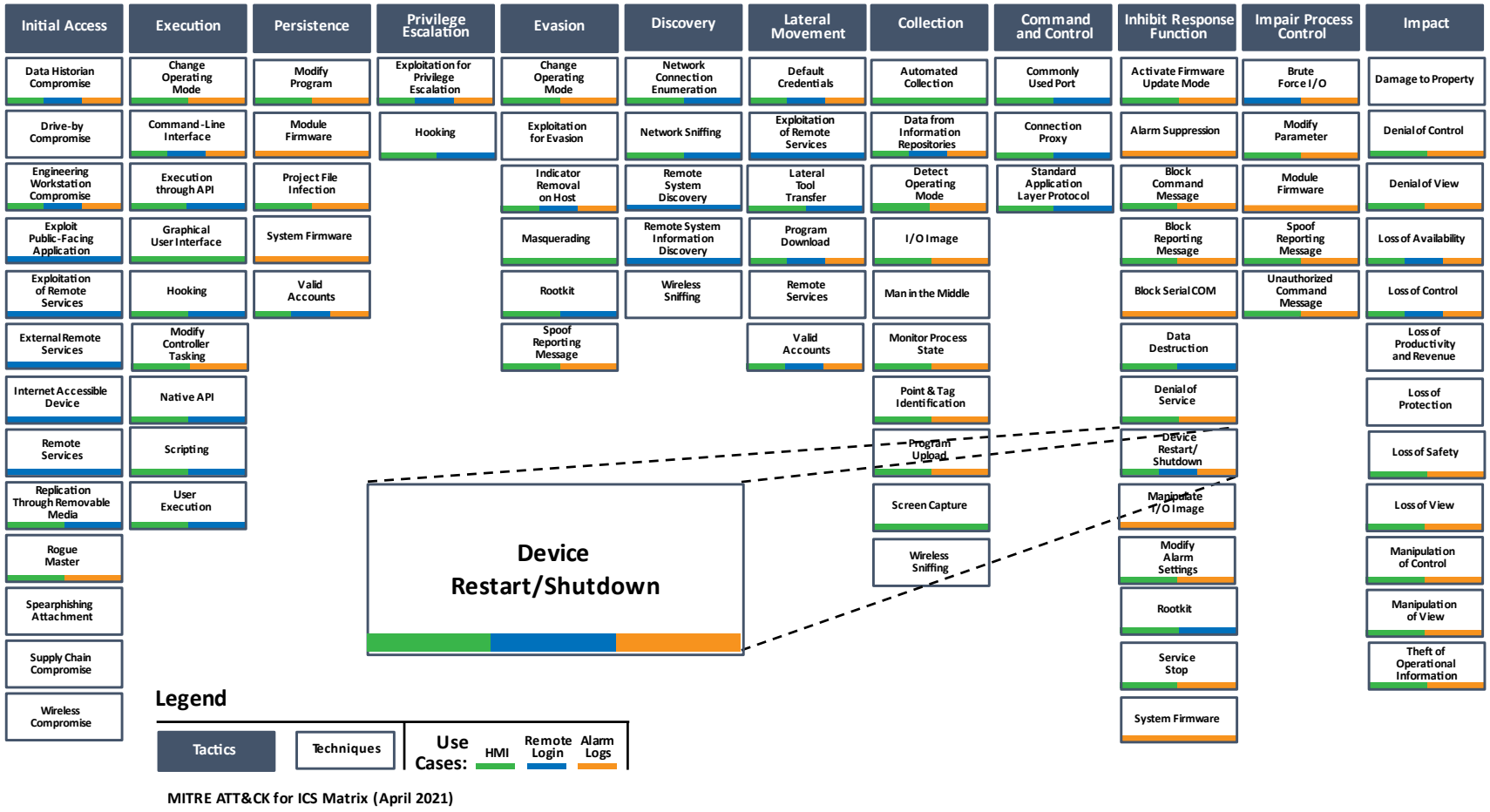


***Figure 1: ICS ATT&CK Framework[9] – Device Restart/Shutdown Technique***

[9] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.